

U.S. Application No. 09/940,982

REMARKS**RECEIVED
CENTRAL FAX CENTER****OCT 16 2006**

The Applicants request reconsideration of the rejection.

Claims 1-8 remain pending.

The Examiner objected to the disclosure for a minor error on page 31, lines 24-26. The Applicants have amended this paragraph of the specification to address the Examiner's concern.

A new Terminal Disclaimer accompanies this Reply to correct the error in the prior, unacceptable Terminal Disclaimer.

Thus, the outstanding rejection of claims 1-8 on the ground of nonstatutory obviousness-type double patenting is overcome. Please note that the Applicants do not admit to the propriety of the double patenting rejection, but submit the Terminal Disclaimer to expedite the allowance of the application.

Claims 1-8 were also rejected under 35 U.S.C. §103(a) as being unpatentable over the Applicants' Admitted Prior Art (AAPA) in view of Jaffe et al., U.S. Patent No. 6,510,518 (Jaffe). The Applicants traverse as follows.

On pages 2-3 of the Office Action, the Examiner notes the prior argument that, although Jaffe teaches that data to be processed can have a constant Hamming weight, there is no suggestion in Jaffe to make constant the Hamming weight for the disturbance data XI or for the processed disturbance data XO recited in the claims. In response, the Examiner states that Jaffe's teaching of constant Hamming weights "would reasonably suggest that the constant Hamming weight representation would be used for all data in a system, including both the 'data to be processed' and the 'data for disturbance' in the admitted prior art."

In this regard, although it appears that the Examiner believes that the teaching of Jaffe is thus applicable any time data needs to be made undecipherable,

the Examiner seems to recognize such an interpretation may be overly broad; and thus asserts that if one were to represent the "data to be processed" in a constant Hamming weight representation, but use a traditional representation for the "data for disturbance", then the two representations would be incompatible because there would not be bit-to-bit correspondence of logical values due to the longer representations in the constant Hamming weight scheme. This seems unfounded, however, since there is no assertion that the disturbance data of AAPA could not be of the same bit length as the input constant-Hamming-mapped data according to Jaffe; rather, it is Jaffe's suggestion that the traditional representation of input data is a single bit which Jaffe maps to two or more bits. Neither Jaffe nor AAPA (nor the Applicants) suggest that the disturbance data must have a different bit length than the input data.

Now discussing the application of Jaffe to AAPA, as admitted on page 21 of the present specification, the prior art has known to transform data to be processed by using data for disturbance. The transformed data D1 is then processed. Finally, a result of the processing is subjected to inverse transformation by using the data for disturbance or by using a result of processing the data for disturbance, to produce data D2 which would also be obtained as a result of performing the processing on the original data. This procedure can be represented as follows:

Input data D1;

Disturb D1 with disturbance data YI;

H1 results;

Process H1;

H2 results;

Disturb H2 with disturbance data YO;

D2 results.

Jaffe teaches to input data to be processed, and then to map the data so as to create data with a constant Hamming weight. Specifically, Jaffe teaches that an input bit 0 is mapped to 01 and an input bit 1 is mapped to 10. The mapped data is processed, and then finally unmapped to produce the result of the processing on the input data. Thus, Jaffe can be represented as follows:

Input data D1;

Map D1;

H1 results;

Process H1;

H2 results;

Unmap H2;

D2 results.

Note that Jaffe does not use disturbance data at any stage, to process D1 into D2.

For this reason, the Applicants earnestly submit that, although Jaffe uses a constant Hamming weight representation for preventing information leakage, it is a precondition that Jaffe essentially does not use disturbance data itself because Jaffe

teaches only the constant Hamming weight representation of the data to be processed, for realizing the stated goal of tamper resistance.

In other words, Jaffe does not include disturbance data itself corresponding to that of the present invention, and there is in fact no need for Jaffe to employ disturbance data corresponding to that of the present invention, because Jaffe's input data is mapped, rather than transformed by data.

Thus, it is difficult to even guess how the person of ordinary skill would employ the teachings of Jaffe in AAPA, other than, perhaps, to suggest that the data to be processed in AAPA is first mapped into a constant Hamming weight representation before being disturbed by the data for disturbance, which does not have a constant Hamming weight. Alternatively, one might argue that the data to be processed according to AAPA is first transformed by using the data for disturbance (not having a constant Hamming weight), and then mapped into a representation having a constant Hamming weight according to Jaffe. However, there appears to be no suggestion or motivation to combine this idea with the AAPA.

Fundamentally, Jaffe does not teach disturbance data or processed disturbance data corresponding to XI and XO of claim 1. Accordingly, claim 1 should be found patentable over the prior art.

Dependent claim 2 has separate patentability. On page 8 of the Office Action, the Examiner asserts that claim 2 is rendered obvious by the Applicants' own admission that the prior art discloses that the processed disturbance data can be generated by carrying out the predetermined processing on the disturbance data used to transform the input data. In fact, however, the AAPA disclosed on page 21 of the present specification states that the inverse transformation is performed by either using the data for disturbance or by "using a result of processing the data for

disturbance". The AAPA does not state that the processing of the data for disturbance used in the inverse transformation is in fact the predetermined processing already performed on the disturbed data itself. Thus, the scope of claim 2 is different from the teaching admitted to be prior art, and is in fact patentably distinct from the prior art.

Dependent claim 3 also has separate patentability. On page 8 of the Office Action, the Examiner asserts that Jaffe discloses that "each bit has a logic value of 1 or 0 at a probability of 50%," citing variable s_8 employed in step 140 of Fig. 1 in Jaffe. Claim 3, however, requires that each bit of the processed disturbance data XO and the disturbance data XI have a logic value of 0 or 1 at a probability of 50%. Variable s_8 of Jaffe is not disturbance data, but is instead an intermediate processing variable used in an exemplary NAND computation process. See column 7, lines 57-59. As noted in lines 59-62, s_8 (and the other intermediate processing variables) are initialized to known states. s_8 thus is not related to the processed disturbance data XO or the disturbance data XI.

Claim 4 is also separately patentable in reciting that the information-processing apparatus further has a disturbance-data and a processed-disturbance-data generation means capable of generating XI with a constant Hamming weight and XO with a constant Hamming weight by execution of input-data processing defined in advance on XI. The Examiner rejects claim 4, asserting again that the applicants have admitted that AAPA discloses generating processed disturbance data by carrying out the predetermined processing on the disturbance data, and that it is well-known that data can be pre-computed. The Applicants have already explained that AAPA does not disclose that XI is processed by any particular

process to obtain XO. Further, the claim does not recite so broadly that "data can be pre-computed".

Concerning claim 5, the Applicants assert separate patentability in the requirement for disturbance-data storage means for storing plural candidates for XI have uniform Hamming weights; and disturbance-data select means for randomly selecting one of the candidates, wherein the disturbance-data processing is carried out to process the selected candidate to generate XO. The Office Action would find this claim obvious over the alleged admission that processed disturbance data can be generated by carrying out predetermined processing on disturbance data, as discussed above, but claim 5 requires significant structure and function not encompassed whatsoever by the passage on page 21. Page 21 does not address storing a plurality of candidates for XI; does not address the random selection of one of the candidates; and does not address processing the disturbance data in accordance with a selected candidate to generate the processed disturbance data. Thus, claim 5 is separately patentable.

Claim 6 is also separately patentable in reciting a constant-Hamming-weight-random-number generation means for generating random numbers with uniform constant Hamming weights, a random-number generation means for generating random numbers each having a Hamming weight equal to half the number of bits in the generated random number, bit inversion means for inverting bits of data, and bit concatenation means for concatenating a random number generated by the random-number generation means with data output by the bit inversion means. The Office Action assert Jaffe and the variable s_8 discussed above. However, s_8 is an intermediate processing variable initialized to a known state, and not generated randomly. Further, column 8, lines 41-45 of Jaffe disclose that variable r_4 is copied

by doubling its length and repeating its value, wherein s_8 is set equal to r_8 and the XOR 11110000. The passage thus does not support the rejection.

Dependent claim 7 recites a random-number generation means for generating a random number to be used as XI, a Hamming weight computation means for computing a Hamming weight of the random number; a Hamming-weight examination means for examining the computed Hamming weight; and a constant-Hamming-weight assurance means for requesting another random number if the examination indicates that the inspected Hamming weight is not equal to a target Hamming weight. Col. 4, line 55 – col. 5, line 30 of Jaffe, cited in the Office Action, discloses that individual bits can be mapped to two-digit binary numbers (or other representations) having constant Hamming weights. There is no suggestion of random number generation, computation of Hamming weights, examination of Hamming weights, or generation of new random numbers to replace insufficient Hamming-weight random numbers. Thus, claim 7 is separately patentable.

Finally, dependent claim 8 has separate patentability in reciting a constant-Hamming-weight and constant-fractional-bit-count random-number generation means for generating partial random numbers with uniform constant Hamming weights and uniform bit counts each equal to a fraction of the bit count of a final random number to be generated; random-number-generation control means for controlling a constant-Hamming-weight and constant-fractional-bit-count random-number generation means to generate partial random numbers until a sum of the bit counts of the partial numbers is equal to the bit count of the final random number; and a data concatenation means for concatenating the partial random numbers thus generated to result in the final random number. The Office Action asserts column 7, line 57 – col. 8, line 65 of Jaffe, which is a discussion of Fig. 1 and the NAND

U.S. Application No. 09/940,982

processing performed therein. However, the NAND processing does not generate constant-Hamming-weight or constant-fractional-bit-count random numbers, does not control the generation of partial random numbers until a sum of bit counts equals the bit count needed for a final random number, and does not concatenate the partial random numbers thus generated to result in the final random number. Indeed, it does not appear that Jaffe employs random number generation of any sort.

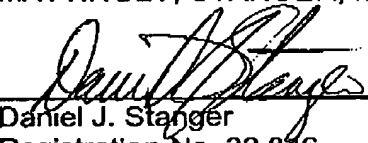
The Applicants request an interview with the Examiner at a mutually-convenient time to discuss these remarks.

In view of the foregoing amendments and remarks, the Applicants request reconsideration of the rejection and allowance of the claims.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Mattingly, Stanger & Malur, P.C., Deposit Account No. 50-1417 (referencing attorney docket no. NIT-295).

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.


Daniel J. Stanger
Registration No. 32,846

DJS/sdb
(703) 684-1120